Google LLC's Motion for Summary Judgment

Redacted Version of Document Sought to be Sealed

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Sara Jenkins (CA Bar No. 230097)
sarajenkins@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Andrew H. Schapiro (admitted *pro hac vice)*
andrewschapiro@quinnemanuel.com
Teuta Fani (admitted *pro hac vice*)
teutafani@quinnemanuel.com
Joseph H. Margolies (admitted *pro hac vice*)
josephmargolies@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
Crystal Nix-Hines (CA Bar No. 326971)
crystalnixhines@quinnemanuel.com
Alyssa G. Olson (CA Bar No. 305705)
alyolson@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Josef Ansorge (admitted *pro hac vice)*
josefansorge@quinnemanuel.com
Xi ("Tracy") Gao (CA Bar No. 326266)
tracygao@quinnemanuel.com
Carl Spilly (admitted pro hac vice)
carlspilly@quinnemanuel.com
1300 I Street NW, Suite 900
Washington D.C., 20005
Telephone: (202) 538-8000
Facsimile: (202) 538-8100

Counsel for Defendant Google LLC
Additional counsel on signature pages

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA, OAKLAND DIVISION

CHASOM BROWN, *et al.*, individually and on behalf of all similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 4:20-cv-03664-YGR-SVK

GOOGLE LLC'S MOTION FOR SUMMARY JUDGMENT

Hon. Yvonne Gonzalez Rogers
Courtroom: 1 – 4th Floor
Date: May 12, 2023
Time: 1:00 p.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Rules

Statutory Authorities

NOTICE OF MOTION AND MOTION

PLEASE TAKE NOTICE THAT, on May 12, 2023, at 1:00 p.m., before the Honorable Yvonne Gonzalez Rogers of the United States District Court for the Northern District of California at the Oakland Courthouse, Courtroom 1, 4th Floor, 1301 Clay Street, Oakland, CA 94612, Defendant Google LLC ("Google") will and hereby does move for an order entering summary judgment in favor of Google on each of Plaintiffs' and Class Members' causes of action. This motion is based upon this Notice of Motion and Motion, the incorporated memorandum of points and authorities, the declaration of Stephen A. Broome, other documents on file in this action, and other evidence and argument presented to the Court.

ISSUE PRESENTED

Whether the Court should grant summary judgment in Google's favor on each of Plaintiffs' and Class Members' causes of action.

RELIEF REQUESTED

Google respectfully requests that the Court grant summary judgment in Google's favor on each of Plaintiffs' and Class Members' causes of action with prejudice.

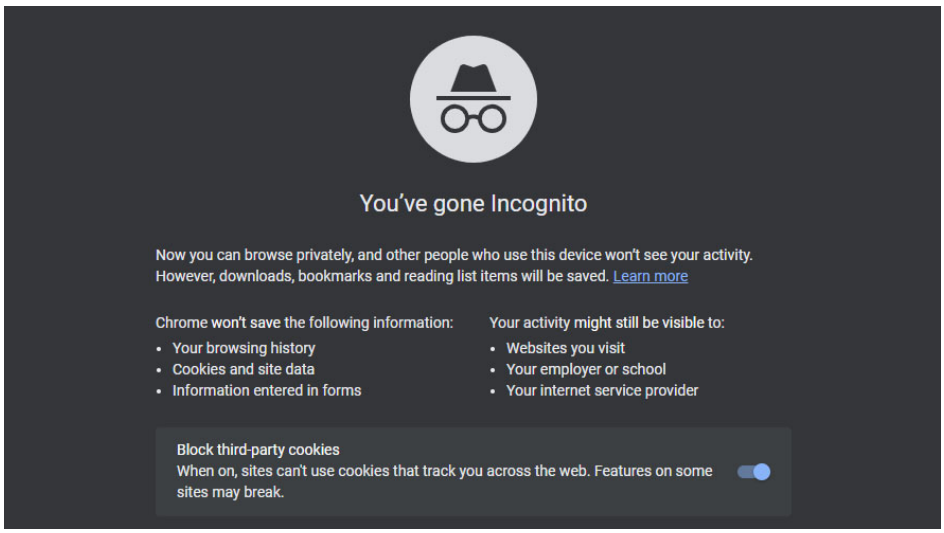
I. INTRODUCTION

Plaintiffs' entire case is based on a simple premise—that Google "promise[d]" that when users were in private browsing mode ("PBM"), Google "would not collect and use private browsing data." Dkt. 886 (FAC) ¶ 271. But nearly three years of extensive discovery has confirmed that Google never made any such promise. To the contrary, it is undisputed that Plaintiffs consented to Google's Privacy Policy—which expressly disclosed the challenged data collection and use—and that PBM provides precisely the degree of privacy described in Google's disclosures. In short, Plaintiffs manufacture from a patchwork of inferences a promise that Google did not make and they ignore both the actual text of Google's disclosures regarding PBM and their own consent to the at-issue data collection. Their claims fail as a matter of law.

First, Plaintiffs and Class Members lack Article III standing because the purported "harm" to their privacy interests is non-existent. To overcome Google's accurate disclosures and their own consent to the data collection, Plaintiffs concocted a theory—matching their allegations to language

used by the Ninth Circuit in *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020)—that Google used PBM data to create "cradle-to-grave profiles" associated with known Google Account holders (*i.e.*, a joined list of an identified user's browsing activity from private and non-private sessions). FAC ¶¶ 89–93. Years of extensive discovery[1] have now thoroughly disproved this theory, confirming that Google's policies and technical safeguards prevent such associations, and that the facts of this case are diametrically opposed to those in *Facebook Tracking*. Indeed, Plaintiffs cannot point to *a single instance* in which Google associated PBM data with Class Members' Google Accounts or otherwise with their identities. They have suffered no harm.

Second, Google never represented that PBM would prevent the routine data collection described in Google's Privacy Policy (*i.e.*, the data Google receives via HTTP resource requests when users visit websites that installed Google's services). Instead, Google accurately explained that Chrome's Incognito mode and other browsers' PBMs provide privacy-enhancing features—*e.g.*, deleting browsing history, cookies and site data locally from the browser—that ensure both local privacy (from users of the same device) and that the data Google receives is not associated with the user's identity or device. Discovery has conclusively established that Incognito works exactly as described. Indeed, Incognito users are reminded *every time* they initiate an Incognito session that Incognito provides privacy from "other people who use this device," but "[y]our activity



[1] Google responded to [redacted] RFPs, [redacted] RFAs, [redacted] interrogatories, produced nearly [redacted] pages, and [redacted] of data. Plaintiffs experts inspected Google's source code and 50 Google witness depositions provided Plaintiffs with [redacted] of testimony. Broome Decl. ¶ 147.

might still be visible to" entities online, including "web-services" that provide "ads and resources" to websites.[2] Users are thus aware that Incognito does not make them invisible while browsing.

Third, discovery confirmed that each named Plaintiff and Class member expressly consented to the relevant Data collection and its use for advertising through Google's Privacy Policy and Account Holder Agreements.[3] The Privacy Policy and Account Holder Agreements disclose that Google collects the at-issue data when users visit websites choosing to use Google services and that Google may use the data for advertising. Express consent defeats all asserted claims.

Because that broad consent is undisputed, Plaintiffs can advance their claims only by identifying a representation by Google that the disclosed data collection would *not* occur when users are in PBM. But there is no such representation. Instead, Plaintiffs' case hinges on tenuous inferences they claim to have drawn from Google's use of the words "private" and "control" to describe PBM. Their inferences are unsupported by the record and cannot overcome the relevant agreements and disclosures—particularly given that Plaintiffs' own privacy expert admits that PBM *does* provide privacy and control, including with respect to Google.

For these reasons and those that follow, the Court should enter judgment in Google's favor.

II. BACKGROUND

A. Private Browsing Modes Offer Users Privacy and Control

When internet users visit websites that have chosen to install Google services that serve ads, conduct analytics, and perform other functions to enhance their sites, Google receives data necessary to provide those services through industry-standard HTTP resource requests. SUF 9. Plaintiffs acknowledge Google's receipt of this data is "common knowledge" and Plaintiffs and Class Members do not deny that they consented to it. SUF 6, 8, 12, 14. Rather, they claim that Google represented that PBM would prevent this process.

[2] The box at the bottom of the Incognito Screen (pictured *supra*) entitled "Block third-party cookies" was added in June and July 2020. Broome Decl. Ex. 85 ¶ 72.

[3] Both classes are limited to Google Account Holders who used a PBM while signed-*out* of their Google Account. Class 1 consists of signed-out Incognito users; Class 2 consists of signed-out users of Safari, Edge, and Internet Explorer PBMs. Dkt. 803 at 24.

PBMs are not intended to prevent web-service providers (like Google) from receiving data to provide their services. Rather, PBM is a browser feature designed to provide users with *local* privacy from other users of the same device (*e.g.*, a spouse, roommate, or child). For example, Chrome's PBM, Incognito, prevents Chrome from saving sites visited during the session in the "History" tab, and deletes cookies, site data, and information entered in forms from the browser when the user closes the Incognito session. SUF 59. Other PBMs do the same. SUF 60.

Google is clear with Chrome users that Incognito "cannot make you invisible on the internet." SUF 26. Nonetheless, in addition to local privacy, Incognito does more to provide users substantial privacy online by ensuring that the data Google receives during an Incognito session is not associated with the user's identity or device, or with data from their other browsing sessions. How it does so is undisputed. First, enabling Incognito automatically logs a user out of her Google Account (and any other online accounts), so that her Incognito activity is not saved there and associated with her identity. SUF 54–55. Second, the browser creates a new, empty "cookie jar" specifically for the PBM session. SUF 50. This separate cookie jar ensures that any data Google receives during a PBM session will not include data associated with previously set cookies. SUF 51. Because Google stores data using unique identifiers contained in cookies (and would not receive any previously set cookies from an Incognito user), SUF 47, the Incognito user appears to Google as a new, unidentified device. When the user closes the Incognito session, Chrome permanently deletes from the browser all cookies placed during that session, preventing Google and other web-services from connecting the data received during the PBM session with the user, her device, or her other browsing activity. SUF 57. The result is that the data Google receives during an Incognito session is both unidentified and "orphaned." *Id.* Google has long-standing policies and technical safeguards preventing Google from linking the "unauthenticated" data it receives when users are in PBM to the users' Google Accounts, their identities, or with their other browsing data. SUF 63.

Other PBMs work similarly to provide users privacy by segregating data from their PBM sessions from the user's identity or device. SUF 60. Indeed, when Plaintiffs subpoenaed Apple, Mozilla, and Microsoft for documents sufficient to "identify all individuals" who used their PBMs, they gave the same response: no such documents exist. SUF 74. Plaintiffs did not pursue it further.

That Incognito and other PBMs provide privacy is not in dispute. Indeed, Plaintiffs' privacy expert, Bruce Schneier, admits that PBMs provide users with both privacy and control.

> Q. And you understand that this is how Incognito and other private browsing modes work; right? That they delete cookies when you close the browser?
> A. Yes.
> Q. And therefore, they do provide a measure of privacy; correct?
> A. I believe I've said that, yes.
> . . .
> Q. Do you agree that by providing a browser mode that prevents the sharing of existing cookies with websites [as Incognito does], Google provides the user with some control?
> A. . . . Yes, that [] gives users some control.
> Q. And do you agree that a browser mode that deletes cookies automatically when you close it [as Incognito does] provides users some control?
> A. Yes.

SUF 75–81. Plaintiff Castillo also admitted that PBMs provide privacy by concealing activity from other people who use the same device. SUF 75.

B. Google's Disclosures Accurately Describe Incognito

Google has never represented that Incognito or other PBMs prevent it from receiving the at-issue data. SUF 1. Nor could it, since the data is necessary to provide services to websites choosing to install Google's code. SUF 90. If PBM blocked all data transmissions to Google (or other web-service providers), useful services that people use every day—including in PBM—would not function.[4] *Id.* Rather, Google explained that Incognito provides certain privacy-enhancing functionalities while simultaneously making clear its limitations. SUF 23, 26, 28, 35, 39, 42. Discovery confirmed the accuracy of each of Google's disclosures.

1. The Incognito Screen

The Incognito Screen is a full-page notice that Chrome displays each time a user enables Incognito. It states, "[n]ow you can browse privately, *and other people who use this device won't see your activity*," SUF 28 (emphasis added), and accurately explains that in Incognito, "Chrome won't save" information ordinarily stored locally—like browsing history and cookies. *Id.* Plaintiffs'

[4] For example, Google Ads would not display; Google Maps would not appear; and the millions of websites that use Google's Analytics services would have an incomplete picture of their website utilization. Further, Google has no ability to stop non-Chrome PBMs (Class 2) from sending data to Google because PBMs are designed not to indicate whether a user is in PBM. SUF 68.

privacy expert testified that this "local privacy" is important to the many users who share their devices. SUF 76. When asked why he did not use PBM himself, he responded, "I never used a shared computer." SUF 77. Thus, even Plaintiffs' own privacy expert understands that people use PBM for local privacy—exactly as Google describes each time a user opens an Incognito window.

The Incognito Screen also makes clear that privacy in Incognito has limits, because "[y]our activity may still be visible" to entities online, including websites, employers, and ISPs. SUF 28. Other browsers' splash screens do the same.[5] SUF 87–89. The Incognito Screen identifies *categories* of entities that may see the user's activity, not specific companies (like Google). The record explains why. Not only would enumerating all entities that could potentially see a PBM user's activity be impossible, but specifically naming Google could create the false impression that unenumerated companies that *also* provide services via HTTP requests do *not* receive the data. SUF 29. In any event, robust, unrebutted survey evidence establishes that changing the Incognito Screen to name "Google" has no statistically significant effect on users' likelihood of using Incognito. SUF 83. This evidence confirms that disclosing that Incognito browsing activity is visible to numerous categories of third parties conveys that PBMs do not provide absolute privacy, including as to Google.

The Incognito Screen provided interested users with even more insight into PBM by including a "Learn more" button that users clicked more than [redacted] times between August 1, 2016 and January 1, 2022. SUF 33. For half the class period, the button linked to the How private browsing works in Chrome page in the Google Help Center, which users visited about [redacted] times between its launch in July 2017 and January 2022. SUF 34, 36. That page explains that "Incognito mode stops Chrome from saving your browsing history to your local history," but "[y]our activity . . . might still be visible to," among others: "websites you visit, including the ads and resources used on those sites"; "Search engines" and "web-service[s]." SUF 35; *see also* Dkt. 803

[5] For example, Firefox explains that its PBM "helps you obscure your online activity from other people who use Firefox on your computer, but does not make you invisible online." SUF 87. And Microsoft explains that "Websites can still personalize content for you during your InPrivate browsing session because cookies and other site permissions aren't deleted until you close all InPrivate windows." SUF 88.

(Class Cert. Order) at 31. Plaintiffs admit it is "common knowledge" that Google provides "ads and resources" to websites and that Google receives the at-issue data as a result. SUF 12, 37.

Since May 2020, the "Learn more" button has linked to the How Chrome Incognito keeps your browsing private page, which was visited about [redacted] times between May 1, 2020 and January 2022. SUF 38, 40. That page similarly explains the local privacy that Incognito provides: "In Incognito, none of your browsing history, cookies and site data, or information entered in forms are saved *on your device*. This means your activity doesn't show up in your Chrome browser history, so people who also use your device won't see your activity." SUF 39. It further explains "[w]hat Incognito mode *doesn't* do," including that Incognito does not "[p]revent the websites you visit from serving ads based on your activity during an Incognito session." *Id.*

2. The Chrome Privacy Notice

The Chrome Privacy Notice ("Chrome Notice") described Incognito mode as follows:

> You can limit the information Chrome stores *on your system* by using incognito mode or guest mode. In these modes, Chrome won't store certain information, such as: [] Basic browsing history information . . . .
>
> **Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new cookies on your system while you are in these modes, but they'll only be stored and transmitted until you close the incognito or guest window.

SUF 23 (emphasis added). The Chrome Notice explains that Incognito limits what "*Chrome* stores on *your* system." Like the Incognito Screen's statement that "*Chrome* won't save" certain data in Incognito, the Chrome Notice is accurate, and that snippet cannot reasonably be interpreted as a promise that Incognito prevents *Google* from receiving the at-issue data. Among other things, "Google" and "Chrome" are not synonymous. Chrome (a downloadable web browser) is just one of Google's many different offerings, and the Chrome Notice uses the terms differently. *See* SUF 24 ("You can stop *Chrome* from accepting cookies *from Google* or other sites. Learn more."); *id.* ("*Chrome* periodically sends information *to Google* to check for updates … [etc.]"). Plaintiffs challenge the collection of data stored on Google's systems, not their own.

The Chrome Notice links to the Chrome Privacy Whitepaper, which explains that Incognito "is a temporary browsing mode. It ensures that you don't leave browsing history and cookies *on your computer*. The browsing history and cookies are deleted only once you have closed the last

incognito window. *Incognito mode cannot make you invisible on the internet*." SUF 26 (emphasis added). Again, these truthful statements do not suggest that Incognito prevents the data collection.

3. Google's Privacy Policy

The Privacy Policy said nothing about Incognito or PBM until May 2018. SUF 19. Google then added a single reference in an introductory paragraph about how users can "manage [their] privacy" across Google's many services "in a variety of ways" including "brows[ing] the web privately using Chrome in Incognito mode." SUF 20. The Privacy Policy *does*, however, thoroughly describe the at-issue data collection and use, SUF 11–14, as this Court found in *Calhoun v. Google LLC*, 2022 WL 18107184, at *10–11, *13 (N.D. Cal. Dec. 12, 2022). Nowhere does the Privacy Policy state that Incognito or other PBMs block the data collection. SUF 18.

C. Google Made No Actionable Statements Regarding Non-Chrome PBMs

Likewise, Google's disclosures do not misrepresent the function of *non-Chrome* PBMs (Class 2). SUF 2. The *only* document Plaintiffs cite describing the functionality of non-Chrome PBMs—and thus potentially applicable to Class 2—is Google's Search & browse privately Help Center page. That Help Center page describes browsers Google did not design and does not control. Accordingly, it makes no "promises" or otherwise actionable statements. Rather, it accurately explains that PBM "*usually* means" that "[t]he searches you do or sites you visit won't be saved *to your device or browsing history*." SUF 42 (emphasis added); *see also id.* (PBM allows you to "search the web without saving your search activity *to your account*"). And like Google's other disclosures, the Search & browse privately page makes clear that PBMs do not provide absolute privacy. It explains that users in PBM may still see "search results and suggestions based on your location or other searches you've done *during your current browsing session*." *Id.* (emphasis added).

D. Plaintiffs and Class Members Expressly Consented to the Contested Data Collection and Its Use

For all browsing modes other than PBM, there is no dispute that Plaintiffs consented to Google's relevant data collection, SUF 3–14, which is precisely the same data collection at issue in the related *Calhoun* case. That collection, which occurs regardless of which browser a user chooses, is governed by Google's Privacy Policy and Account Holder Agreements. *See Calhoun*, 2022 WL

18107184, at *10 ("Because the . . . at-issue data collected is not specific to Chrome but browser agnostic, . . . Google's general policies apply.").[6]

This Court has found that Google's Privacy Policy discloses its collection and use of the data. *Id.* at *11; SUF 11. Plaintiffs admit the same, acknowledging that (1) the data collection is "common knowledge," SUF 12; (2) they were aware of it before filing suit, SUF 13; (3) the Privacy Policy is part of their contract with Google, SUF 15; and (4) they consented to the data collection for all browsing modes other than PBM, SUF 14. With these facts undisputed, the only question is whether Google represented that PBMs *prevented* the data collection, thereby *negating* Plaintiffs' consent when using them. There is no genuine dispute: Google made no such representation.

III. ARGUMENT

A. Plaintiffs and Class Members Lack Article III Standing

Plaintiffs fail to establish that Google's conduct caused Class Members to suffer an injury sufficient for Article III standing. Discovery has confirmed that Plaintiffs' allegations (FAC ¶¶ 54, 69, 91–112) that Google built "cradle-to-grave profiles" that "associate" PBM data "with the user's 'Google profile,'" are false. Instead, the record confirms that the "orphaned" data at issue is never associated with users' identities and that doing so would be impossible without overriding Google's policies and technical safeguards preventing such linking. SUF 49–51, 54–57, 62–66. Thus, the asserted "harm" to Class Members' privacy interests is non-existent.[7] *See Cahen v. Toyota Motor*

[6] Plaintiffs' allegations concerning the data collection by Google for both Class 1 (Incognito PBM) and Class 2 (Non-Chrome PBMs) are identical. *See generally* FAC. Accordingly, Plaintiffs concede that the data collection is browser-agnostic and Google's general policies apply.

[7] The Ninth Circuit's decision in *Facebook Tracking* does not hold otherwise—indeed, it provides a point of contrast. There, the Court found standing for privacy claims based on allegations that Facebook made "affirmative statements that it would not receive information from third-party websites after users had logged out," but continued to collect logged out users' data and "correlat[e] users' browsing history with users' *personal Facebook profiles*—profiles that could include a user's employment history and political and religious affiliations," giving Facebook "a cradle-to-grave profile without users' consent." *Facebook Tracking*, 956 F.3d at 596–99 (emphasis added). Here, the evidence conclusively proves the at-issue data is *not* associated with users' identities. The Ninth Circuit also found standing for certain claims requiring economic injury, including CDAFA, based on Facebook's alleged "unjust enrichment." *Id.* at 599–02. But here, unjust enrichment is not an available remedy for the Rule 23(b)(2) classes and therefore cannot satisfy Article III's requirement

Corp., 717 F. App'x 720, 724 (9th Cir. 2017) (holding defendants' collection of "non-individually identifiable driving history and vehicle performance data" was insufficient to "cause an actual injury" for Article III purposes); *I.C. v. Zynga, Inc.*, 2022 WL 2252636, at *1049 (N.D. Cal. Apr. 29, 2022) (Gonzalez Rogers, J.) (no standing for privacy, contract, and other claims where plaintiffs' "anonymity is preserved" and the "pieces of information" revealed to third parties, on their own, were not "so private that their revelation would be highly offensive"); *Low v. LinkedIn Corp.*, 2011 WL 5509848, at *4 (N.D. Cal. Nov. 11, 2011) (no standing where plaintiff failed to allege "his browser history will be linked to his identity by LinkedIn" or "how third party advertisers will be able to infer his personal identity from his anonymous LinkedIn user ID").

Unable to show Google links the at-issue data to their identities, Plaintiffs and their experts have pivoted to assert that Google has the *capability* to do so. SUF 66. But given Google's undisputed policies and technical safeguards against such linking, SUF 63–64, Plaintiffs cannot show that "the risk of harm is sufficiently imminent and substantial" to confer standing for damages or injunctive relief. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2209–12 (2021).

B. Each Claim Fails Because Plaintiffs and Class Members Expressly Consented to Google's Collection and Use of the Data

"He who consents to an act is not wronged by it." Cal. Civ. Code § 3515. Lack of consent is Plaintiffs' burden to prove for certain asserted claims,[8] and consent is a defense to all the others. *See Calhoun*, 2022 WL 18107184, at *8 (consent is a defense to wiretapping, privacy, breach of contract, and UCL claims); *Calhoun v. Google*, 526 F. Supp. 3d 605, 620 n.3 (N.D. Cal. 2021) ("Consent is [] a defense to Plaintiffs' breach of contract" and "UCL claim").

It is undisputed that *each* Plaintiff reviewed and consented to the Privacy Policy. SUF 3–4, 6. It is also undisputed that the Privacy Policy (1) governs and discloses the at-issue data collection

---

that the alleged injury "is likely to be redressed by a favorable judicial decision." *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016).

[8] *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 828 (N.D. Cal. 2020) ("the plaintiff bringing a CIPA claim has the burden to prove that the defendant lacked consent"); 18 U.S.C. § 2511(2)(d) (consent exception); Cal. Penal Code § 502(c) ("without permission" is an element of CDAFA claim); *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 26 (1994) ("the plaintiff in an invasion of privacy case ... must not have manifested by his or her conduct a voluntary consent").

(SUF 7, 11), and (2) discloses that Google uses the data for advertising and other purposes. *See supra* II.B.3; *Calhoun*, 2022 WL 18107184, at *10–11, 13 (quoting portions of Google Privacy Policy that disclose the data collection and use). Thus, Plaintiffs can avoid summary judgment only if they can show a genuine issue as to whether Google represented PBM would block all data transmissions to Google. Google never made such representations.

The Privacy Policy *never* carved out Incognito or PBM from its thorough disclosures about the data collection. In fact, when each Plaintiff consented to it (between 2004 and 2012, SUF 5), the Privacy Policy mentioned neither Incognito nor PBM. *Supra* II.B.3. There is simply no basis to understand the Privacy Policy to suggest the data collection described would be blocked in PBM.

In May 2018, *years after* Plaintiffs consented to the Privacy Policy, Google added a single reference to Incognito in a prefatory paragraph stating that users can "use [Google's] services in a variety of ways to manage your privacy," including by "brows[ing] the web privately using Chrome in Incognito mode." SUF 20. Even if Plaintiffs had gone back and reviewed the amended Privacy Policy years after consenting to it, no one could reasonably have understood that to be a promise that Incognito blocks all transmissions of data to Google—*because the Privacy Policy does not say that*. Rather, it describes Incognito as one way to manage your privacy online, which it indisputably is. This accurate characterization of Incognito as a "private" mode is plainly insufficient to negate Plaintiffs' and Class Members' undisputed consent to the data collection.

The Incognito Screen further undermines Plaintiffs' effort to avoid their consent to the data collection. It makes clear each time Incognito launches that Incognito provides privacy from "other people who use this device," and that while "*Chrome* won't save" certain information to the user's browser in Incognito mode (*e.g.*, browsing history, cookies and site data, information entered in forms), the user's activity may still be visible to entities online.[9] SUF 28. The Incognito Screen

[9] Without a plausible argument to negate consent in the Privacy Policy that undisputedly governs the data collection, Plaintiffs argue that class members understood the phrase "Chrome won't save . . . ." in the Incognito Screen, and "Chrome won't store . . . ." in the Chrome Notice, to mean that *Google* would not *receive* the Data. Dkt. 192 (MTD Opp.) at 11 n.6; Dkt. 609 (Class Cert. Mot) at 9. But there is no evidence (other than Plaintiffs' self-serving testimony) to support that atextual reading of Google's disclosures. Nor would any such reading be reasonable, given that—as shown

features a "Learn more" button that, from July 2017 to May 2020, displayed a detailed article on How private browsing works in Chrome. SUF 34. As the Court recognized in its Class Certification Order, that article makes clear that while Incognito "stops Chrome from saving your browsing history *to your local history*," "[y]our activity … might still be visible to . . . websites you visit, including the ads and resources used on those sites . . . [s]earch engines . . . and web-service[s]." *See* Dkt. 803 at 31. That is important because Plaintiffs admit they were aware Google receives data through its provision of "web-services" that deliver "ads and resources" to websites.[10] SUF 37. Since May 2020, the "Learn more" button has linked to a different article that makes similarly robust disclosures about how Incognito works and its limitations. SUF 38–39.

Because it is undisputed that Incognito provides privacy and control in the manner described in Google's disclosures, there is no basis for negating Plaintiffs' admitted consent to the data collection described in the Privacy Policy, and all claims should be dismissed. *See Smith v. Facebook, Inc.*, 745 F. App'x 8, 8–9 (9th Cir. 2018); *Calhoun*, 2022 WL 18107184, at *13.

C. Plaintiffs' and Class Members' Claims Should Be Dismissed for Additional Reasons

1. Breach of Contract (Count 6)

Even beyond their lack of standing and their express consent, Plaintiffs fail to raise a triable issue for their contract claim. *First*, none of the documents Plaintiffs claim comprise their contract[11] contains the purported "promis[e] that 'private browsing mode' would prevent Google from collecting users' data." Dkt. 609 (Class Cert. Mot.) at 2; Dkt. 192 (MTD Opp.) at 12. That alone

---

above—the disclosures separately define Chrome and Google, and use the terms in a way that makes clear they are *not* the same. *Supra* II.B.

[10] The other disclosures on which Plaintiffs rely do not negate consent to the data collection either. The Chrome Notice describes Incognito mode (and Guest mode) as ways to "limit the information Chrome stores *on your system*." SUF 23. It further explains that "Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new cookies on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window." *Id.* The "Search & browse privately" help center article provides a similar description. SUF 42. These descriptions are indisputably accurate.

[11] Plaintiffs allege their "contract" consists of "the Google Terms of Service, the Google Chrome and Chrome OS Additional Terms of Service, and the Chrome Privacy Notice, which incorporate and/or should be construed consistent with the Privacy Policy, the Search & Browse Privately [Help Center article], and the Incognito Screen." SUF 15.

defeats their contract claim. Under Ninth Circuit authority, to prove breach of contract, Plaintiffs must first identify an "explicit promise" they allege was broken. *Facebook Tracking*, 956 F.3d at 610 (affirming dismissal of contract claim because contract did "not contain an explicit promise not to track logged-out users"); *Hammerling v. Google LLC*, — F. Supp. 3d —, 2022 WL 2812188, at *16 (N.D. Cal. 2022) (dismissing contract claim because "[t]he question is whether Google breached anything that it promised, not whether Google did anything it did not promise"); *Beecher v. Google N. Am. Inc.*, 2018 WL 4904914, at *2 (N.D. Cal. Oct. 9, 2018) (dismissing contract claim where plaintiffs failed to "point to specific contractual terms which were allegedly breached").[12]

Discovery has confirmed the absence of any explicit promise that Google breached. When pressed to identify the allegedly breached representations, Plaintiffs identified only snippets from the four paragraphs below (two of which are from non-contractual documents, *see infra*):

> Post-May 2018 Privacy Policy: "You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used."
>
> Chrome Notice: "You can limit the information Chrome stores on your system by using incognito mode or guest mode. In these modes, Chrome won't store certain information such as: Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit."
>
> Search & browse privately Help page: "You're in control of what information you share with Google when you search. To browse the web privately, you can use private browsing, sign out of your account, change your custom results settings, or delete past activity. If you want to search the web without saving your search activity to your account, you can use private browsing mode in a browser (like Chrome or Safari)."
>
> Incognito Screen: "Now you can browse privately, and other people who use this device

[12] *See also Becton, Dickinson & Co. v. Cytek Biosciences Inc.*, 2020 WL 1877707, at *4 (N.D. Cal. Apr. 15, 2020) (dismissing contract claim where plaintiff failed to "identif[y] … the *particular contractual provision* on which [plaintiff] relies for its assertion that [defendant's] use [of plaintiff's information] is prohibited") (emphasis added); *Murphy v. Allstate Ins. Co.*, 2020 WL 5095862, at *2 (E.D. Cal. Aug. 28, 2020) (dismissing contract claim because plaintiff "fails to identify the *specific provision* of the policy that the defendant breached") (emphasis added); *Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 978 (N.D. Cal. 2016) ("[A] plaintiff must, in actions involving breach of a written contract, allege the *specific provisions* in the contract creating the obligation the defendant is said to have breached.") (emphasis added) (quotation marks and citation omitted).

> won't see your activity… Chrome won't save the following information: Your browsing history[;] Cookies and site data[;] Information entered in forms[;] . . . ."

SUF 21, 25, 30, 43. Not one of these statements "promis[es] that 'private browsing mode' would prevent Google from collecting users' data." Dkt. 608-3 (Class Cert. Mot.) at 2. There is no explicit promise, and thus no viable contract claim. *See Facebook Tracking*, 956 F.3d at 610.

Plaintiffs purport to *infer* a promise from these snippets by applying their subjective interpretation of what it means to "browse privately." But Plaintiffs' subjective understanding is irrelevant to contract interpretation where their contract with Google explains exactly what it means to browse privately, *i.e.*, that Chrome won't save certain information such as basic browsing history information "on *your* system" or share existing cookies with sites you visit. *See Block v. eBay, Inc.*, 747 F.3d 1135, 1138 (9th Cir. 2014) ("It is not the parties' subjective intent that matters, but rather their objective intent, as evidenced by the words of the contract.").

Plaintiffs' argument that some "reasonable users" might agree with their alleged interpretation was enough to survive at the pleading stage, but it falls well short of raising a triable issue of fact at summary judgment. Plaintiffs have adduced no evidence supporting the claim that their alleged interpretation was shared by *anyone*. SUF 84. In fact, the study conducted by Google's survey expert, On Amir, confirms most users who were shown the documents Plaintiffs claim comprise their contract expected that Google "does or probably does" receive the data. SUF 85; Dkt. 803 (Class Cert. Order) at 30. Plaintiffs' survey expert offered no contrary evidence.[13] SUF 84. Nor can Plaintiffs support their allegedly "reasonable" interpretation with their own self-serving testimony. *Krouch v. Wal-Mart Stores, Inc.*, 2014 WL 5463333, at *8 (N.D. Cal. Oct. 28, 2014) (Gonzalez Rogers, J.) ("[T]his court has refused to find a 'genuine issue' where the only evidence

[13] Plaintiffs' survey expert, Mark Keegan, did not test users' understanding of the alleged contract—he tested *only* the Incognito Screen (which is not a contract or part of a contract). *See* SUF 84. And even then, he found that "roughly half of respondents who were asked whether they agreed that Google 'collects and saves' [the at-issue data] in [PBM] confirmed that they did agree, which represents more than three times the number of respondents who disagreed." Dkt. 803 (Class Cert Order), at 30–31. Given the limitations and conclusions of Mr. Keegan's study—and the Court's holding that Plaintiffs' privacy expert, Mr. Schneier, is barred from opining on consumer expectations, *id.* at 17–19—Mr. Amir's evidence is unrebutted.

presented is 'uncorroborated and self-serving' testimony." (quoting *Villiarimo v. Aloha Island Air, Inc.*, 281 F.3d 1054, 1061 (9th Cir. 2002))).

Second, even if there were a triable issue as to the interpretation of the statements above, none of them is an enforceable promise under Ninth Circuit precedent. Even in the context of an otherwise binding user agreement, "provisions [] written in an informal, conversational style, indicating that the agreement is not simply a set of legally enforceable promises, but also an introduction to the [defendant's services] for new users," are not enforceable for breach of contract. *Block*, 747 F.3d at 1138–40. Thus, a document providing "simply a general description of how [the defendant's] system works" cannot be enforced on a contract theory absent explicit "promissory language." *Id.*; *see also Facebook Tracking*, 956 F.3d at 611 (statement in privacy policy that merely "provides information[,] not commitments" is not binding); *Rodriguez v. Google LLC*, 2022 WL 214552, at *3 (N.D. Cal. Jan. 25, 2022) (dismissing contract claim based on Help Center webpage that "merely contains explanatory language about Google's products"). In addition, to be binding, the document must reflect "an *exchange* [of] promise[s]," involving consideration. *Facebook Tracking*, 956 F.3d at 610 (emphasis added).

The portions of the Chrome Notice, Incognito Screen and Search & browse privately page on which Plaintiffs rely do not meet these requirements. There is plainly no "exchange of promises" in these documents; they simply provide information about how Incognito and PBM work. As such, the relevant provisions cannot be enforced through a breach of contract claim. *See Block*, 747 F.3d at 1138–40 (eBay's statement in user agreement that "'We are not involved in the actual transaction between buyers and sellers'—contains no promissory language"; "Rather, the statement is simply a general description of how eBay's auction system works" and thus not enforceable).

Nor do the snippets relied upon by Plaintiffs from the post-May 2018 Privacy Policy give rise to an enforceable promise. These statements appear in an introductory paragraph generally describing various ways that users can manage their privacy across Google's diverse services. As Judge Breyer recently found, such statements "are not express promises, but aspirational and prefatory statements." *Hammerling v. Google LLC*, 2022 WL 17365255, at *11 (N.D. Cal. Dec. 1, 2022) (dismissing similar claims for alleged breach of Google's Privacy Policy); *see also*

Block, 747 F.3d at 1138–40. Further, the Privacy Policy's description of Incognito as a "private" mode does "not actually bind Google to offer any particular privacy settings" or functionality. *Rodriguez v. Google LLC*, 2021 WL 6621070, at *3 (N.D. Cal. Aug. 18, 2021). And even if that statement somehow did extend a promise, it would be breached only if Incognito provided "no control whatsoever" over users' privacy. *Id.* (dismissing contract claims based on Google privacy disclosures for similar reasons); *see also In re Google Location History Litig.* 514 F. Supp. 3d 1147, 1160 (N.D. Cal. 2021) (dismissing similar contract claim based on Google's Privacy Policy); *Rodriguez*, 2022 WL 214552, at *3 (same). That is not the case. Plaintiffs' own privacy expert admits Incognito provides privacy and control. SUF 75–82. Therefore, even assuming the Privacy Policy statements were enforceable, the record confirms Google has not breached them.

Third, neither the Incognito Screen nor the Search & browse privately Help page is a stand-alone contract or part of a contract and cannot support a claim for breach. Plaintiffs argue that the documents are "incorporated by reference" into the Terms of Service and the Chrome Notice. FAC ¶ 268. But documents "incorporated by reference" in a contract must be "clear[ly] and unequivocal[ly]" incorporated with an "explicit" reference. *See Shaw v. Regents of Univ. of Cal.*, 58 Cal. App. 4th 44, 53–54 (1997); *Facebook Tracking*, 956 F.3d at 610 (rejecting incorporation of document that was not explicitly referenced); *Rodriguez*, 2021 WL 6621070, at *4 (Google's "Help Page is not incorporated by reference into the Privacy Policy"). Neither the Incognito Screen nor the Help Page is referenced in the Terms of Service or the Chrome Notice. SUF 32, 46. And Plaintiffs' argument that these documents are incorporated by reference into the Privacy Policy fails because neither document is referenced there either. The mere fact that Incognito *mode* is mentioned in the Privacy Policy (starting May 2018) "is not the same as specifically directing the parties' attention to the terms of the [Incognito *Screen*] in a manner that could be construed as eliciting the parties' consent to its separate terms." *Amtower v. Photon Dynamics, Inc.*, 158 Cal. App. 4th 1582, 1608–09 (2008). Given that neither the Terms of Service, the Chrome Notice, nor the Privacy Policy reference the Incognito Screen or the Search & browse privately Help page, those documents cannot be incorporated by reference to support a contract claim.

Fourth, the *only* document that references PBM generally, rather than Incognito specifically—and thus the only document potentially applicable to Class 2—is the Search & browse privately Help page which, as shown above, is not contractual and makes no "promises."

Finally, the contract claim should be dismissed as to both Classes because it has been certified solely to seek injunctive relief, which is "explicitly unavailable in contract actions." *RSI Corp. v. Int'l Bus. Machines Corp.*, 2012 WL 3277136, at *7 (N.D. Cal. Aug. 9, 2012); Cal. Civ. Code. § 3423 ("An injunction may not be granted . . . [t]o prevent the breach of a contract the performance of which would not be specifically enforced . . . .").[14]

2. Federal Wiretap Act Interception Claim (Count 1)

a. Websites Consented to Google's Receipt of the Data

Plaintiffs' claim fails because the Wiretap Act is a one-party consent statute, 18 U.S.C. § 2511(2)(d), and the intended recipients of the alleged communications—websites that installed Google's code—consented to Google's receipt of the at-issue data. Indeed, the purpose of installing the code is to send the data to Google to obtain its services. SUF 90–97, 100.

Because "the consent of one party is a complete defense," the websites' consent is fatal to Plaintiffs' Wiretap Act claim.[15] *Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021). Chief Judge Seeborg's decision in *Rodriguez*—another case Plaintiffs' counsel is pursuing against Google—is directly on point. Chief Judge Seeborg held that Google could not be

[14] Even Plaintiffs' latest amendment to their complaint—for the purposes of clarifying the relief they seek for each claim—does not seek specific performance. Dkt. 886 (FAC), Prayer for Relief. Nor could they seek this remedy given it requires a showing of inadequacy of legal remedy and that the promise to be enforced is indeed contained in the contract (here it is nowhere to be found). *Lewis v. YouTube, LLC*, 244 Cal. App. 4th 118, 126 (2015).

[15] The consent exception does not apply where the communications at issue are "intercepted for the purpose of committing any criminal or tortious act," but that "exception to the exception" plainly does not apply here. *In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218, at *12 (N.D. Cal. Dec. 22, 2022). "[T]he focus [of the crime-tort exception] is not upon whether the interception itself violated another law; it is upon whether the *purpose* for the interception—its intended use—was criminal or tortious." *Sussman v. ABC, Inc.*, 186 F.3d 1200, 1202–03 (9th Cir. 1999) (internal quotation marks omitted); *Rodriguez*, 2021 WL 2026726, at *6 n.8 (crime-tort exception "cannot apply where the interceptor's 'purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.'") (quoting *In re Google Inc. Gmail Litigation*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014)).

liable under the Wiretap Act for "intercept[ing]" app activity data because the intended recipients of the data—app developers—installed Google's code for the *purpose* of transmitting the data to Google, and therefore consented. *Id.* at *5–6. Indeed, courts in this Circuit and beyond treat such voluntary installation as creating a *presumption* of consent.[16]

Plaintiffs asserted at the pleading stage that websites did not consent to Google's receipt of the data while users are in PBM. But that argument has been exposed as a paper tiger. The record confirms that websites consent to Google's receipt of the data *generally*, and that their consent does not depend on a user's browsing mode. SUF 92. Plaintiffs produced no contrary evidence.

Moreover, even if Plaintiffs had raised a triable issue about whether *class members* reasonably understood PBM to block all data transmissions to Google, they cannot substitute that purported expectation for those of more technologically sophisticated website developers. Chief Judge Seeborg correctly rejected as "untenable" the argument that *users'* purported expectations of privacy affect *developers'* consent to Google's receipt of data. *Rodriguez*, 2021 WL 2026726, at *5 ("Common sense [] coupled with plaintiffs' omission of any caselaw charting a contradictory course, disposes of the 'consent-upon-consent' theory.").

b. Google Received the Data in the Ordinary Course of Business

Plaintiffs' Wiretap Act claim also fails because Google received the data in the ordinary course of business. A defendant may be liable under the Wiretap Act only for intercepting communications through use of a wiretapping "device," which excludes technology "being used by a provider of wire or electronic communication service in the ordinary course of business." *See* 18

[16] *See In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218, at *12 (no Wiretap Act liability because "healthcare providers who configured [Meta's code] on their websites presumably consented to Meta's receipt of the information"); *Cohen v. Casper Sleep, Inc.*, 2018 WL 3392877, at *1–2 (S.D.N.Y. July 12, 2018) (dismissing Wiretap Act claims where "[h]undreds of online retailers entered into voluntary partnerships with [an activity tracking company] to insert [its] Code into their websites"); *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 509–11 (S.D.N.Y. 2001) ("find[ing] it implausible to infer that the Web sites have not authorized DoubleClick's [n.k.a. Ad Manager] access" since "the very reason clients hire DoubleClick is to target advertisements based on users' demographic profiles"); *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153, 1160–62 (W.D. Wash. 2001) ("It is implicit in the web pages' code instructing the user's computer to contact [defendant] . . . that the web pages have consented to [defendant]'s interception of the communication between them and the individual user.").

U.S.C. §§ 2510(5)(a) & 2511(1). Here, the alleged intercepting "device" is the Google code that websites install on their sites to obtain Google's services, which causes the user's browser to send the data to Google's servers. SUF 91. There is no dispute that Google and websites use that code (and related infrastructure) in the ordinary course of the business of online advertising, analytics, and other web-services. SUF 93–97.

Courts have held the ordinary course of business exception provides a "broad immunity" protecting all of a service provider's "customary and routine business practices," *In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *10–11 (N.D. Cal. Dec. 3, 2013), or more narrowly to:

> offer[] protection from liability 'only where an electronic communication service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication' and there is 'some nexus between the need to engage in the alleged interception and the [provider's] ultimate business, that is, the ability to provide the underlying service or good.

Matera v. Google Inc., 2016 WL 8200619, at *14 (N.D. Cal. Aug. 12, 2016) (quoting *In re Google Inc. Gmail Litigation*, 2013 WL 5423918, at *8, 11 (N.D. Cal. Sept. 26, 2013)). Either way, the requisite nexus is present here. Websites engage Google's services specifically to facilitate the user-website interactions at issue. After all, a website is an amalgam of first- and third-party content and functions, and for the third-party content (*e.g.*, an ad, a Google Map, Google Fonts) to appear, an HTTP request to the third-party's servers is required. SUF 97. Thus, the "device" at issue here (Google's code) is essential for websites to function as their developers intended.[17]

c. The Data Is Not "Contents" of a Communication

Plaintiffs' claim fails for yet another reason. The Wiretap Act "only applies to the interception of the 'contents' of a communication." *In re Carrier IQ, Inc. Consumer Privacy Litig.*, 78 F. Supp. 3d 1051, 1082 (N.D. Cal. 2015) (citing 18 U.S.C. § 2510(4)). "Contents" means "information concerning the substance, purport, or meaning of th[e] communication," 18 U.S.C. § 2510(8)—in other words, "the intended message conveyed by the communication," *In re Zynga*

[17] In *Matera*, the court found an insufficient nexus because the plaintiffs plausibly alleged that scanning emails to serve targeted advertising does not "facilitate the provision of email services, [and is] not an incidental effect of providing those services." 2016 WL 8200619, at *14. Here, by contrast, the record establishes that websites could not use Google's services without installing Google code that cause the data to be sent to Google in order to retrieve the relevant services.

Privacy Litig., 750 F.3d 1098, 1106 (9th Cir. 2014). Emails, text messages, and similar communications contain "contents." *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1034 (N.D. Cal. 2014) (Gonzalez Rogers, J.). Under Ninth Circuit authority, the data here does not.

Plaintiffs invoke the Wiretap Act by alleging Google illicitly "intercepted" record data by way of HTTP requests when they visited websites using Google's services: (a) GET requests with referer headers (a type of HTTP request); (b) IP addresses; (c) information identifying users' browser configuration; (d) "any 'User-ID' issued by the website to the user"; (e) location (if available); and (f) "[i]nformation contained in 'Google cookies'" (*i.e.*, identifiers issued by Google). FAC ¶ 63(a)–(f). The Ninth Circuit's decision in *Zynga* is dispositive: neither "ID[s that] identif[y] a [] user," nor "HTTP referrer information" that includes the "webpage address [that] identifies the location of a webpage a user is viewing," qualify as "contents." 750 F.3d at 1106–07. Rather, the data is merely "record information" that "Congress excluded . . . from the definition of 'contents.'" *Id.* at 1105–07; *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. 2021) (*Zynga* establishes that "contents" does *not* include "keystrokes, mouse clicks, pages viewed, . . . the date and time of the visit, the duration of the visit, Plaintiffs' IP address, her location at the time of the visit, her browser type, and the operating system on her device").[18]

3. Cal. Penal Code §§ 631 & 632 ("CIPA") (Count 2)

Like their Wiretap Act claim, Plaintiffs' § 631 claim fails because they fail to prove Google intercepted "contents" of communications from the Class. *See Brodsky*, 445 F. Supp. 3d at 127 ("The analysis for a violation of CIPA [§ 631] is the same as that under the federal Wiretap Act."); Cal. Penal Code. § 631(a) (requires interception of "the contents or meaning" of a communication).

[18] *See also Russo v. Microsoft Corp.*, 2021 WL 2688850, at *4 (N.D. Cal. June 30, 2021) ("documents, contacts, and calendar information" not "contents"); *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *14 (N.D. Cal. Feb. 2, 2021) ("data on when and how often an Android Smartphone user opens and runs non-Google apps and the amount of time spent on the apps" not contents under *Zynga*); *Brodsky*, 445 F. Supp. 3d at 127 ("user names, passwords, and geographic location information" not "contents"); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1034 ("name, address, email address or phone number" are not "contents").

Plaintiffs' § 632 claim should be dismissed because discovery has conclusively established that the allegedly intercepted "communications" (HTTP requests) are not "confidential" under the statute, which excludes communications made under "any [] circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." Cal. Penal Code § 632(c); *see also Flanagan v. Flanagan*, 27 Cal. 4th 766, 768 (2002). Simply put, a "communication" is not actionable under the statute if there is any reasonable expectation that it may be (1) "*overheard*" by anyone, other than the websites a user visits, or (2) "*recorded*" by anyone, *including* the websites. Discovery has established both are true here.

Plaintiffs admit they understood from the Incognito Screen that their activity would be visible to their Internet Service Provider and their employer or school. SUF 98. Their awareness of third parties having access to their alleged communications is dispositive. Even more, Plaintiffs knew their activity would be visible to the websites they visit, SUF 98–99, and thus reasonably should have expected that it would be recorded by the websites. Indeed, "California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of section 632, because such communications can easily be shared by . . . the recipient(s) of the communications [*e.g.*, the websites]." *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014); *Rodriguez*, 2021 WL 2026726, at *7 (dismissing § 632 claim notwithstanding plaintiffs' alleged expectation that *Google* would not record their communications with third party apps because that expectation "does not reasonably give rise to the expectation that *nobody* (including the apps' developers) would record the communications") (emphasis in original).[19]

4. California Penal Code § 502(c)(2) ("CDAFA") (Count 3)

Plaintiffs' claim under California's anti-hacking statute should be dismissed because it is

[19] *See also Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) ("[I]n California, courts have developed a presumption that Internet communications do not reasonably give rise to th[e] expectation [that the conversation is not being overheard or recorded].") (collecting cases); *In re Google Inc. Gmail Litigation*, 2013 WL 5423918, at *22 ("California appellate courts ... suggest that internet-based communication cannot be confidential . . . [because] individuals cannot have a reasonable expectation that their online communications will not be recorded."); *People v. Nakai*, 183 Cal. App. 4th 499, 518–19 (2010) (criminal defendant's intent to keep his internet chats confidential did not satisfy § 632(a) because it was reasonable to assume that the communications could be recorded or shared by the service provider).

undisputed that: (1) Google did not "access" Plaintiffs' computers, and (2) Plaintiffs have not suffered "damages or loss."[20]

First, Google did not "access" Plaintiffs' computers as that term is defined in Cal. Penal Code § 502(b)(1).[21] The undisputed process at issue involves third-party website developers' downloading and installing code on their websites that directs the browsers of users visiting their sites to send an HTTP request to Google servers. SUF 100. Google is not responsible for installing the code; it merely receives data in order to provide the service requested. SUF 93–96, 101. Such "'reactive' data collection, logging and sending to [defendant] data that users receive from [plaintiff] through their normal use of the website" does not fall within CDAFA's scope. *Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1260–62 (N.D. Cal. 2022) (granting summary judgment on part of CDAFA claim concerning data collection from third parties); *see also New Show Studios LLC v. Needle*, 2014 WL 2988271, at *6–8 (C.D. Cal. June 30, 2014) (dismissing CDAFA claim because "[a]ccessing plaintiffs' information…is not the same thing as accessing plaintiffs' computer systems, even if that information was at some point stored on those computers."). Any broader interpretation of CDAFA's "access" requirement is unreasonable—and would be inconsistent with the rule of lenity—because it would criminalize routine internet functionality.

Second, Plaintiffs suffered no "damage or loss by reason of a violation." Cal. Pen. Code § 502(e)(1); *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950–51 (N.D. Cal. 2014) (dismissing CDAFA claim for failure to plead damage or loss); SUF 102–104. Plaintiffs' alleged "loss of the right to control their own data, the loss of the value of their data, and the loss of the right to protection of the data … is [not] 'damage or loss' within the meaning of the CDAFA." *Cottle v. Plaid Inc*., 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021); *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at

[20] Cal. Penal Code § 502(c)(2) provides in relevant part: "[A]ny person who commits any of the following acts is guilty of a public offense: … (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network."

[21] Cal. Penal Code § 502(b)(1) provides: "'Access' means to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network."

*4-5 (N.D. Cal. Nov. 20, 2020); *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1050 (N.D. Cal. 2018) (dismissing CDAFA claim in the absence of "deprivation of income or actual loss").

5. Invasion of Privacy and Intrusion Upon Seclusion (Counts 4 and 5)

The privacy claims fail for reasons beyond consent and lack of standing. Courts analyzing claims for invasion of privacy and intrusion upon seclusion "consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Facebook Tracking*, 956 F.3d at 601. Neither element is satisfied here.

The only reasonable privacy expectation Plaintiffs and Class Members could have is that Incognito and other PBMs perform the specific, privacy-enhancing functions described in Google's disclosures, which they indisputably do. Even if Google had not explained PBMs' limitations in its disclosures, courts hold there is no expectation of privacy in the type of unidentified data at issue.[22]

Nor can Plaintiffs show that Google's collection and use of the data is "highly offensive"—which would require showing that the "invasion[] of privacy [is] sufficiently serious in [its] nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill v. Nat'l Coll. Ath. Ass'n.*, 7 Cal. 4th 1, 37 (1994). Indeed, "[m]any courts have found that the collection . . . of personal information about the users of a technology may not constitute a sufficiently 'egregious breach of social norms' to make out a common law or constitutional privacy claim." *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 830

[22] *See, e.g.*, *Sanchez v. Los Angeles Dep't of Transportation*, 2021 WL 1220690, at *3 (C.D. Cal. Feb. 23, 2021), *aff'd*, 35 F.4th 721 (9th Cir. 2022), *aff'd*, 39 F.4th 548 (9th Cir. 2022) ("Obviously, a person does not have a reasonable expectation of privacy over information that cannot even be connected to her."); *Hammerling*, 2022 WL 2812188 at *12–13 n.11 (dismissing privacy claims where no allegations that "the personal information collected by Google is non-aggregate or de-anonymized"); *Hammerling*, 2022 WL 17365255, at *9 (dismissing privacy claims where plaintiffs failed to plausibly allege Google used the data "to develop comprehensive profiles on its users") (internal quotations omitted); *Moreno v. S.F. Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017) (dismissing privacy claims based on "[d]efendants' periodic transmitting to their servers of [plaintiff's] *anonymous* clientid . . . and location); *U.S. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) ("Internet users have no expectation of privacy in . . . IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").

(collecting cases).[23] Moreover, Plaintiffs admit they continued using Incognito after filing suit despite being aware of the data collection and use, and have taken no other steps to prevent Google from receiving the data. SUF 105–106. Since people ordinarily do not subject themselves to "highly offensive" conduct, Plaintiffs' continued use of PBM after filing suit belies their allegation.

6. Unfair Competition Law ("UCL") (Count 7)

a. Plaintiffs Lack UCL Standing

The undisputed record confirms that Plaintiffs lack standing for their UCL claim because they have not "lost money or property." Cal. Bus. & Prof. Code § 17204. Plaintiffs have not lost money because they paid nothing to use Chrome or the other at-issue browsers. SUF 102; *see Wesch v. Yodlee, Inc.,* 2021 WL 1399291, at *6 (N.D. Cal. Feb. 16, 2021) (dismissing UCL claim for lack of standing because plaintiffs "have not paid Yodlee any money").

Nor have Plaintiffs lost property. *See* SUF 103–104. The Ninth Circuit has held that, for information to constitute property, it must be "capable of exclusive possession or control." *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003). The data at issue here is not capable of exclusive possession and control by Class Members; it is designed to be routinely exchanged to facilitate internet communications. For example, the fact that a user read an article on nytimes.com cannot be "possessed" by the user, let alone "exclusively possessed," given the New York Times receives the same information. Accordingly, the Ninth Circuit and courts in this District consistently hold that such information does not constitute property for purposes of the UCL's heightened standing requirement. *See, e.g.*, *In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) ("personal information" allegedly disclosed by Facebook does not constitute "lost money or property" under the UCL); *In re Zynga Privacy Litig.*, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011), *aff'd,* 750 F.3d 1098 (9th Cir. 2014) ("personal information does not constitute property for purposes of a UCL claim"); *Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 603–04 (N.D.

[23] *See also Moreno*, 2017 WL 6387764, at *8 (collection of anonymous geolocation data not "an egregious breach of social norms"); *In re Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 121–23 (W.D. Pa. 2019) ("The act of collecting [plaintiff's] keystrokes, mouse clicks, and PII is simply not the type of highly offensive act to which [intrusion upon seclusion] liability can attach.").

Cal. 2021) ("private geolocation data" is not "lost money or property . . . under the UCL").[24]

b. Plaintiffs Have an Adequate Remedy at Law

The UCL claim also fails because Plaintiffs have an adequate remedy at law. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020) (plaintiff "must establish that she lacks an adequate remedy at law before securing equitable restitution for past harm under the UCL"); *Guzman v. Polaris Indus. Inc.*, 49 F.4th 1308, 1312 (9th Cir. 2022) (same); *Shay v. Apple Inc.*, 2021 WL 1733385, at *3 (S.D. Cal. May 3, 2021) ("[D]istrict courts have held that the 'adequate remedy at law' requirement applies to equitable relief, which includes injunctive relief claims," and collecting cases).[25] This requirement remains "even if all of plaintiff's non-UCL claims ultimately fail." *Moss v. Infinity Ins. Co.*, 197 F. Supp. 3d 1191, 1203 (N.D. Cal. 2016); *Guzman,* 49 F.4th at 1312; *Rhynes v. Stryker Corp.*, 2011 WL 2149095, at *4 (N.D.Cal. May 31, 2011) (same). Here, Plaintiffs seek legal remedies based on contract, statutory, and tort theories. Courts routinely dismiss UCL claims where privacy plaintiffs also allege such claims for legal remedies.[26]

IV. CONCLUSION

For the foregoing reasons, the Court should grant Google's motion for summary judgment and dismiss all claims asserted by Plaintiffs and the Class.

---

[24] *See also Cottle*, 536 F. Supp. 3d at 483–85 (even personal banking information not "lost money or property"); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1093 (N.D. Cal. 2018) ("[S]haring of names, user IDs, location and other personal information does not constitute lost money or property for UCL standing . . . ."); *Claridge v. RockYou*, 785 F. Supp. 2d 855, 863 (N.D. Cal. 2011) (personal information cannot be "'lost' . . . under the UCL. . . . [P]laintiff's PII—e.g., his login and password information—did not cease to belong to him, or pass beyond his control").

[25] *See also Browning v. Am. Honda Motor Co.*, 549 F. Supp. 3d 996, 1014 (N.D. Cal. 2021) ("since Plaintiffs have not pled that they lack an adequate remedy at law, all their equitable claims, including those for restitution and prospective injunctive relief, fail"); *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 662 (N.D. Cal. 2020) ("Cases in this Circuit have held that *Sonner* extends to claims for injunctive relief"); *Clark v. Am. Honda Motor Co.*, 528 F. Supp. 3d 1108, 1121–22 (C.D. Cal. 2021) (dismissing UCL claim seeking "prospective injunctive relief" under *Sonner*); *Audrey Heredia v. Sunrise Senior Living LLC*, 2021 WL 819159, at *4 (C.D. Cal. Feb. 10, 2021) (similar).

[26] *See, e.g.*, *Veritas Techs. LLC v. Cushman & Wakefield, Inc.*, 2022 WL 222527, at *11 (N.D. Cal. Jan. 25, 2022) (granting judgment on the pleadings as to UCL claim because it failed to plead that a remedy at law was inadequate when it also sought damages for conversion and breach of contract); *Luckett v. Kohl's Dep't Stores, Inc.*, 2020 WL 4341779, at *6 (C.D. Cal. June 18, 2020) (granting summary judgment on UCL claim because "Plaintiff's statutory claims entitle her to damages" and "she [] failed to submit any evidence demonstrating that those remedies are inadequate").

DATED: March 21, 2023

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By: /s/ Andrew H. Schapiro
Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
Teuta Fani (admitted *pro hac vice*)
teutafani@quinnemanuel.com
Joseph H. Margolies (admitted *pro hac vice*)
josephmargolies@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
Crystal Nix-Hines (CA Bar No. 326971)
crystalnixhines@quinnemanuel.com
Alyssa G. Olson (CA Bar No. 305705)
alyolson@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Sara Jenkins (CA Bar No. 230097)
sarajenkins@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
Xi ("Tracy") Gao (CA Bar No. 326266)
tracygao@quinnemanuel.com
Carl Spilly (admitted *pro hac vice*)
carlspilly@quinnemanuel.com
1300 I. Street, N.W., Suite 900
Washington, D.C. 20005
Telephone: 202-538-8000
Facsimile: 202-538-8100

Jomaire A. Crawford (admitted *pro hac vice*)
jomairecrawford@quinnemanuel.com
D. Seth Fortenbery (admitted *pro hac vice*)
sethfortenbery@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC